CLAIM AMENDMENTS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently amended) A method ~~for~~ of detecting intrusion in a host via a monitoring daemon operating in conjunction with a configuration file defining data entities to be monitored, ~~said~~ the method ~~as implemented in said host~~ comprising ~~the steps of~~:

[[a.]]monitoring ~~said~~ data entities via comparing a locally stored copy of a digital signature associated with each data entity against a corresponding digital signature stored in a first remote database; and

[[b.]]upon identifying a mismatch in compared digital signatures, issuing an instruction to record an entry in a log file located in a second remote database, said entry identifying a possible intrusion in ~~said~~ a host.

2. (Currently amended) ~~A~~ The method ~~for detecting intrusion in a host via a monitoring daemon operating in conjunction with a configuration file defining data entities to be monitored,~~ ~~as per~~ of claim 1, ~~wherein said host communicates with said first and second remote databases via one or more network interfaces and, subsequent to step (b), said method~~ further ~~comprises the step of~~ comprising issuing a command to bring down said one or more network interfaces to isolate said host upon identifying the mismatch in compared digital signatures.

3. (Currently amended) ~~A~~ The method ~~for detecting intrusion in a host via a monitoring daemon operating in conjunction with a configuration file defining data entities to be monitored,~~ ~~as per~~ of claim 1, ~~wherein, subsequent to step (b), said method~~ further ~~comprises the step of~~ comprising issuing a command to an operating system of the host to bring said host to a single user state upon identifying the mismatch in compared digital signatures.

4. (Currently amended) ~~A~~ The method ~~for detecting intrusion in a host via a monitoring daemon operating in conjunction with a configuration file defining data entities to be monitored,~~

~~as per~~ of claim 1, wherein said first remote database and said second remote database are located on a single server or a plurality of servers belonging to a local area network.

5. (Currently amended) ~~A~~ The method ~~for detecting intrusion in a host via a monitoring daemon operating in conjunction with a configuration file defining data entities to be monitored, as per~~ of claim 1, wherein communications between said host and first remote database are encrypted.

6. (Currently amended) ~~A~~ The method ~~for detecting intrusion in a host via a monitoring daemon operating in conjunction with a configuration file defining data entities to be monitored, as per~~ of claim 1, wherein communications between said host and second remote database are encrypted.

7. (Currently amended) ~~A~~ The method ~~for detecting intrusion in a host via a monitoring daemon operating in conjunction with a configuration file defining data entities to be monitored, as per~~ of claim 1, wherein said digital signature is an MD5 signature and said first remote database is an MD5 database.

8. (Currently amended) ~~A~~ The method ~~for detecting intrusion in a host via a monitoring daemon operating in conjunction with a configuration file defining data entities to be monitored, as per~~ of claim 1, wherein said second remote database is a SYSLOG database.

9. (Currently amended) ~~A~~ The method ~~for detecting intrusion in a host via a monitoring daemon operating in conjunction with a configuration file defining data entities to be monitored, as per~~ of claim 1, wherein said data entities comprise one or more ~~are any~~ of ~~the following:~~ system files, configuration files, ~~or~~ and directories.

10. (Currently amended) A system to detect intrusion comprising:

[[a.]]a host running a monitoring daemon working in conjunction with a configuration file, said configuration file identifying files and directories to be monitored in said host and said host communicating with external networks via one or more network interfaces, said monitoring daemon dynamically monitoring said files and directories identified by said configuration file by comparing a locally stored digital signature corresponding to each file or directory against a remotely stored corresponding digital signature;

[[b.]]a digital signature database remote from said host storing said digital signatures associated with files and directories identified by said configuration file; and

[[c.]]a log database remote from said host recording entries corresponding to mismatches between a digital signature stored in said host and a corresponding digital signature in said digital signature database.

11. (Currently amended) ~~A~~ The system to detect intrusion as per claim 10, wherein said ~~first remote~~ digital signature database and said log ~~second remote~~ database are located on a single server or a plurality of servers belonging to a local area network.

12. (Currently amended) ~~A~~ The system to detect intrusion as per claim 10, wherein communications between said host and said digital signature database are encrypted.

13. (Currently amended) ~~A~~ The system to detect intrusion as per claim 10, wherein communications between said host and log database are encrypted.

14. (Currently amended) ~~A~~ The system to detect intrusion as per claim 10, wherein said digital signature is an MD5 signature and said first remote database is an MD5 database.

15. (Currently amended) An article of manufacture comprising a computer usable medium having computer readable program code ~~embed~~ embedded therein to detect intrusion in a host via a monitoring daemon operating in conjunction with a configuration file defining data entities to be monitored, said medium comprising:

[[a.]]computer readable program code comprising executable instructions to monitor ~~monitoring said~~ data entities via comparing a locally stored copy of a digital signature associated with each data entity against a corresponding digital signature stored in a first remote database; and

[[b.]]~~upon identifying a mismatch in compared digital signatures,~~ computer readable program code comprising executable instructions to issue ~~issuing~~ an instruction to record an entry in a log file located in a second remote database upon identifying a mismatch in compared digital signatures, said entry identifying a possible intrusion in ~~said~~ a host.

16. (Currently amended) ~~An~~ The article of manufacture as per claim 15~~, wherein said host communicates with said first and second remote databases via one or more network interfaces and said medium~~ further ~~comprises~~ comprising computer readable program code comprising executable instructions to issue ~~issuing~~ a command to bring down ~~said~~ one or more network interfaces to isolate said host upon identifying the mismatch in compared digital signatures.

17. (Currently amended) ~~An~~ The article of manufacture, as per claim 15~~, wherein said method~~ further ~~comprises~~ comprising computer readable program code comprising executable instructions to issue ~~the step of issuing~~ a command to an operating system of said host to bring said host to a single user state upon identifying the mismatch in compared digital signatures.

18. (Currently amended) An intrusion detection and isolation method implemented using a monitoring daemon in a host, said host having one or more network interfaces to communicate over one or more networks, said method comprising ~~the steps of~~:

[[a.]]reading a configuration file to identify data entities to be monitored on a host;

[[b.]]for each data entity to be monitored, extracting a digital signature from said host;

[[c.]]for each data entity to be monitored, querying a remote digital signature database via said one or more network interfaces and requesting a digital signature corresponding to said digital signature extracted from said host;

[[d.]]for each data entity to be monitored, receiving said corresponding digital signature from said remote digital signature database;

[[e.]]matching digital signature received from said remote digital signature database with digital signature extracted at said host;

[[f.]]upon identifying a mismatch, transmitting an instruction to a remote log database via said one or more network interfaces, said instruction executed in said remote log database to record an entry in a log file indicating a possible intrusion in said host; and

[[g.]]performing ~~any~~ at least one of~~, or a combination of,~~ the following ~~steps~~:

[[(i)]]issuing a command to bring down said one or more network interfaces to isolate said host; ~~or~~ and

[[(ii)]]issuing a command to an operating system of host to bring said host to a single user state.

19. (Currently amended) The ~~An~~ intrusion detection and isolation method implemented using a monitoring daemon in a host, as per claim 18, wherein said digital signature database and said log database are located on a single server or a plurality of servers belonging to a local area network.

20. (Currently amended) The ~~An~~ intrusion detection and isolation method implemented using a monitoring daemon in a host, as per claim 18, wherein communications between said host and digital signature database are encrypted.

21. (Currently amended) The ~~An~~ intrusion detection and isolation method implemented using a monitoring daemon in a host, as per claim 18, wherein communications between said host and log database are encrypted.

22. (Currently amended) The ~~An~~ intrusion detection and isolation method implemented using a monitoring daemon in a host, as per claim 18, wherein said digital signature database is an MD5 database.

23. (Currently amended) The ~~An~~ intrusion detection and isolation method implemented using a monitoring daemon in a host, as per claim 18, wherein said log database is a SYSLOG database.

24. (Currently amended) The ~~An~~ intrusion detection and isolation method implemented using a monitoring daemon in a host, as per claim 18, wherein said data entities are any of the following: system files, configuration files, or directories.